

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 244 270 A2

(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:

25.09.2002 Patentblatt 2002/39

(51) Int Cl.7: **H04L 29/06**

(21) Anmeldenummer: **02002845.2**

(22) Anmeldetag: **08.02.2002**

(84) Benannte Vertragsstaaten:

**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR**

Benannte Erstreckungsstaaten:

AL LT LV MK RO SI

(30) Priorität: **22.03.2001 DE 10114156**

(71) Anmelder: **Deutsche Telekom AG**

53113 Bonn (DE)

(72) Erfinder:

- **Milczewsky, Klaus**
64342 Seeheim-Jugenheim (DE)
- **Boos, Elmar**
97906 Faulbach (DE)

(54) **Verfahren zur Bereitstellung eines authentischen elektronischen Zertifikats**

(57) Die Erfindung betrifft ein Verfahren zur Bereitstellung eines authentischen elektronischen Zertifikats. Ihr liegt die Aufgabe zugrunde, ein Verfahren anzugeben, durch welches solche Zertifikate schnell und kostengünstig bereitgestellt werden können.

Die Aufgabe wird durch eine Automatisierung der Verifikationsvorgänge für die zur Erzeugung verwendeten Identitätsmerkmale eines das Zertifikat anfordernden Nutzers gelöst. Ein das Zertifikat generierender und in eine Public-Key-Infrastruktur eingebundener Server greift dazu auf Identitätsmerkmale zurück, welche in ei-

nem in seinem Zugriff befindlichen Speicher auf der Grundlage eines bereits bestehenden, elektronisch abgebildeten Vertragsverhältnisses gespeichert wurden und im Hinblick auf das bestehende Vertragsverhältnis als vertrauenswürdig eingestuft werden können. Gemäß einer möglichen Ausgestaltung greift der Server mittels einer inversen RADIUS-Abfrage auf bei einem Internet Service Provider gespeicherte Vertragsdaten zu.

EP 1 244 270 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Bereitstellung eines authentischen elektronischen Zertifikats, bei welchem das Zertifikat von einem Client unter Nutzung einer elektronischen Verbindung bei einem Server angefordert werden kann, der Server das angeforderte Zertifikat automatisch generiert und es an den Client überträgt.

[0002] Mit der zunehmenden Verbreitung elektronischer Medien für die Datenübertragung bzw. Datenfernübertragung, insbesondere mit der zunehmenden Nutzung des Internet für derartige Zwecke steigt der Bedarf an Möglichkeiten zur Gewährleistung der Vertraulichkeit und der Authentizität der übertragenen Daten. Vertrauliche Daten werden daher vor der Übertragung mittels kryptographischer Verfahren verschlüsselt. Dabei werden für offene Systeme wie das Internet sogenannte asymmetrische Verschlüsselungsverfahren bevorzugt, bei denen für das Verschlüsseln einer Nachricht (von Daten) ein anderer Schlüssel eingesetzt wird als für das Entschlüsseln. Soweit der für das Verschlüsseln verwendete Schlüssel ein öffentlich bekannter Schlüssel (Public Key) ist, spricht man in diesem Zusammenhang auch von Public-Key-Verfahren. Derjenige, der den öffentlichen Schlüssel bekannt gibt, kann dabei von einer Mehrzahl unterschiedlicher Absender Nachrichten erhalten, welche von allen Absendern mit dem öffentlichen Schlüssel verschlüsselt werden, aber nur durch den Empfänger mit seinem persönlichen und geheimen Schlüssel zu entschlüsseln sind. Auf diese Weise ist die Vertraulichkeit der übertragenen Nachrichten gewährleistet. Im Hinblick darauf, dass der Nutzer eines offenen Systems, in welchem er Daten mit anderen Nutzern austauscht, wechselnd Absender und Empfänger von Nachrichten ist, verfügt jeder Nutzer, der diese Daten vertraulich unter Nutzung des Public-Key-Verfahrens austauschen möchte, über einen eigenen, den anderen Kommunikationspartner bekanntzugebenden öffentlichen Schlüssel und über mehrere öffentliche Schlüssel anderer Nutzer sowie über einen privaten Schlüssel. Aus Performancegründen werden zur Verschlüsselung größerer Nachrichten auch so genannte hybride Verfahren eingesetzt, bei denen die Nachricht selbst mit einem schnellen symmetrischen Verschlüsselungsalgorithmus (z.B. DES - siehe hierzu z.B. Beutelspacher, Schwenk, Wolfenstetter "Moderne Verfahren der Kryptographie", 3. Auflage Vieweg Verlag Wiesbaden 1999) verschlüsselt wird, und dann nur der zum Entschlüsseln benötigte symmetrische Schlüssel mit dem öffentlichen Schlüssel des Empfängers bzw. mit den öffentlichen Schlüsseln der Empfänger verschlüsselt und der Nachricht beigelegt wird.

[0003] Allerdings identifiziert der öffentliche Schlüssel allein seinen Nutzer, eine Applikation oder einen Host noch nicht, d.h. der Empfänger der verschlüsselten Nachricht hat keine Gewähr über deren Authentizität, er weiß zum Beispiel nicht, ob der vorgebliche Absender

auch der tatsächliche ist. Um auch hier Sicherheit zu schaffen, bedient man sich eines weiteren kryptographischen Mechanismus, der so genannten digitalen Signatur. Der Nutzer einer digitalen, auch als elektronische Unterschrift bezeichneten Signatur muss dabei bei denen, die später signierte Nachrichten von ihm erhalten, einmalig Vertrauen in die Authentizität dieser elektronischen Unterschrift schaffen. Entsprechend einer einfachen, einen so genannten out-of-band-Mechanismus nutzenden Variante ist die Vorgehensweise hierzu in etwa die folgende: Der Nutzer der digitalen Signatur signiert einen Datensatz, der seinen öffentlichen Schlüssel, Identifikationsinformationen (z. B. seine E-Mail-Adresse) und einen kurzen Hashwert enthält, mit seinem privaten Schlüssel. Nach der Übermittlung der Information ruft er den Empfänger an und gibt ihm telefonisch den verwendeten Hashwert durch. Sofern sich Sender und Empfänger kennen, kann dabei der Empfänger den Absender der Nachricht anhand seiner Stimme identifizieren. Demzufolge kann er auch den Datensatz, sofern dieser nach Entschlüsselung mit dem öffentlichen Schlüssel den ihm zur Kenntnis gegebenen Hashwert enthält, als authentisch erkennen und ihn entsprechend kennzeichnen. Künftig kann er jede auf identische Weise signierte Mitteilung des Empfängers als authentisch einstufen (nähere Einzelheiten hierzu siehe u. a. Beutelspacher, Schwenk, Wolfenstetter "Moderne Verfahren der Kryptographie", 3. Auflage Vieweg Verlag Wiesbaden 1999). Problematisch ist es hierbei, dass zur Gewährleistung der Authentizität ein vergleichsweise hoher Aufwand erforderlich ist. Wollten sich beispielsweise die Mitarbeiter einer Firma mit 1.000 Mitarbeitern auf die beschriebene Weise gegenseitig authentisieren, müsste hierzu jeder Mitarbeiter zumindest einmal mit jedem anderen kommunizieren. Es wären demnach 999.000 Telefonate erforderlich.

[0004] Eine Verbesserung der Situation ergibt sich bei der Verwendung so genannter Public-Key-Infrastrukturen. Hier wird das Vertrauen, also die Authentizität in einer baumförmigen Struktur über- bzw. vermittelt. Die Nutzer müssen lediglich Vertrauen in eine Zertifizierungseinrichtung und das von ihr bereitgestellte so genannte Root-Zertifikat herstellen. Alle anderen Vertrauensbeziehungen der Nutzer untereinander lassen sich dann aus diesem Root-Zertifikat ableiten. Nähere Einzelheiten hierzu siehe beispielsweise <http://www.logosec.de/zertifikate.htm>.

[0005] Bezogen auf das oben genannte Beispiel der Firma mit 1.000 Mitarbeitern wären hier noch etwa 2.000 Verifikationen nötig. Dazu müsste jeder der 1.000 Mitarbeiter das Root-Zertifikat akzeptieren und an einer zentralen Stelle müssten die mit dem jeweiligen öffentlichen Schlüssel verknüpften Identifikationsdaten der Mitarbeiter überprüft und im Erfolgsfall der Datensatz mit dem privaten Schlüssel, welcher dem Root-Zertifikat zugeordnet ist, signiert werden. Ein solches von der zentralen Stelle signiertes Zertifikat würde auf Grund der Vertrauensbeziehung zwischen den Nutzern und

der Zertifizierungsstelle die Authentizität der Mitarbeiter untereinander belegen können. Das Zertifikat ist dabei mit einem elektronischen Personalausweis vergleichbar. Die Erstellung derartiger Zertifikate erfolgt vorzugsweise nach dem X.509-Standard der ISO. Allerdings verursacht die Überprüfung der Identifikationsdaten durch die zentrale Stelle dabei aber immer noch einen beträchtlichen Aufwand. Bei der Verwendung eines out-of-band-Mechanismus müssten die Nutzer beispielsweise zu ihrer Identifizierung ihren Personalausweis oder andere ihre Identität belegende Nachweise vorlegen. Dies ist für den massenhaften Einsatz viel zu aufwendig und letztlich auch zu teuer.

[0006] Aufgabe der Erfindung ist es daher, ein Verfahren anzugeben, durch welches authentische elektronische Zertifikate schnell und kostengünstig bereitgestellt werden können. Die Aufgabe wird durch ein Verfahren entsprechend dem Hauptanspruch gelöst. Vorteilhafte Ausgestaltungen bzw. Weiterbildungen des erfindungsgemäßen Verfahrens sind durch die Unteransprüche gegeben.

[0007] Gemäß der Erfindung wird das Zertifikat von einem Client unter Nutzung einer elektronischen Verbindung bei einem in eine Public-Key-Infrastruktur eingebundenen Server einer Zertifizierungsstelle abgefordert, von diesem Server automatisch generiert und an den Client übertragen. In erfindungswesentlicher Weise generiert dabei der Server das Zertifikat unter Nutzung von Identitätsmerkmalen, welche in seinem Speicher oder in Speichermedien, auf die er über elektronische Verbindungen Zugriff hat, auf der Grundlage eines bereits bestehenden, in dem Speicher oder den Speichermedien elektronisch abgebildeten Vertragsverhältnisses gespeichert sind. Diese Identitätsmerkmale sind im Hinblick auf das bestehende Vertragsverhältnis als vertrauenswürdig einzustufen. Auf Grund einer dem Aufbau der Verbindung mit dem Server vorausgehenden Anmeldeprozedur, welche eine Voraussetzung für den Aufbau der elektronischen Verbindung vom Client zum Server darstellt, stehen die im Zugriff des das Zertifikat generierenden Servers befindlichen Identitätsmerkmale außerdem in einer zumindest vermeintlichen eindeutigen Zuordnung zu dem das Zertifikat mittels des Clients abfordernden Nutzer. In diesem Zusammenhang soll die Formulierung einer vermeintlich eindeutigen Zuordnung lediglich zum Ausdruck bringen, dass natürlich auch an dieser Stelle Manipulationen nicht auszuschließen sind, und zwar dann, wenn beispielsweise der eigentliche Nutzer des Clients seine Zugangsdaten für das Internet einem anderen Nutzer bekannt gibt bzw. überlässt oder wenn sie widerrechtlich durch einen Dritten in Erfahrung gebracht und genutzt werden. Grundsätzlich ist jedoch davon auszugehen, dass auf Grund der Anmeldeprozedur zum Herstellen der Verbindung zwischen dem Client und dem Server vom Nutzer des Clients Angaben abgefordert bzw. Handlungsweisen verlangt werden, in deren Ergebnis die Eindeutigkeit der Zuordnung für den angestrebten Zweck unterstellt wer-

den kann. Der Kerngedanke der Erfindung liegt also darin, den bereits erwähnten aufwendigen out-of-band-Mechanismus zur Überprüfung der Identität des das Zertifikat anfordernden Nutzers durch den elektronischen Rückgriff auf ein bereits bestehendes Vertragsverhältnis zu ersetzen, in dessen Rahmen als authentisch anzusehende Identitätsangaben des Nutzers als elektronische Abbildung des Vertragsverhältnisses abgespeichert wurden. Dem liegt die Überlegung zugrunde, dass personengebundene Daten heute sowieso bereits in vielfältigster und weiterverarbeitbarer Form elektronisch gespeichert werden, wobei dieser Speicherung in vielen Fällen eine Überprüfung auf Authentizität vorangeht. Warum sollte man sich also dieser Tatsache nicht bedienen. Selbstverständlich müssen technische und gegebenenfalls auch organisatorische Voraussetzungen für den Zugriff auf diese Daten geschaffen werden. [0008] Gemäß einer praxisrelevanten Anwendung des Verfahrens handelt es sich bei der elektronischen Verbindung zwischen dem Server und dem Client um eine IP-Verbindung. Eine Ausgestaltung des Verfahrens sieht nun vor, dass die dem Client (und damit seinem Nutzer) bei der Einwahl in das IP-Netz nach dem erfolgreichen Durchlaufen einer hierzu üblichen Anmeldeprozedur zugeteilte temporäre IP-Adresse als zentraler technischer Referenzwert für den Zugriff des das Zertifikat generierenden Servers auf die im Zuge der elektronischen Abbildung des bereits angesprochenen bestehenden Vertragsverhältnisses gespeicherten Identitätsmerkmale dient. Entsprechend einer bevorzugten Ausführungsform für die Verwendung im IP-Netz erfolgt dabei der Zugriff des Servers auf die Identitätsmerkmale unter Umkehr der bei der Einwahl des Clients in das IP-Netz für die Zuweisung der temporären IP-Adresse genutzten Remote Authentication Dial-In User Service-Abfrage (RADIUS-Abfrage). Dabei löst der Server die temporäre IP-Adresse, unter der ihn der Client kontaktiert hat, durch eine inverse RADIUS-Abfrage und eine sich anschließende Datenbankabfrage zu den elektronisch gespeicherten Identitätsmerkmalen und aufgrund des zwischen dem Nutzer und einem Internet Service Provider (ISP) bestehenden Vertragsverhältnisses als authentisch anzusehenden Daten des Nutzers auf. Dies ist möglich, wenn entweder der ISP selbst auch als Zertifizierungsstelle auftritt und er demzufolge auch den Server zur Generierung der Zertifikate betreibt und somit unmittelbaren Zugriff auf die Vertragsdaten hat oder, wenn der ISP dem Server einer als allgemein vertrauenswürdig anerkannten Zertifizierungsstelle diesen Zugriff einräumt.

[0009] Entsprechend einer möglichen Variante des Verfahrens erfolgt die Anmeldeprozedur, also die Einwahl in das IP-Netz über den Server eines ISP, unter Nutzung der Password Authentication Protocol Methode (PAP), so dass der Server unter Anwendung der inversen RADIUS-Abfrage aus der temporären IP-Adresse zuerst auf den Username und gegebenenfalls auf das Password des das Zertifikat anfordernden Nutzers

schlussfolgt und mittels der sich daran anschließenden Datenbankabfrage die (authentischen) Identitätsmerkmale des Nutzers erhält. Da der Username zumindest im Verhältnis zu dem entsprechenden ISP in der Regel eindeutig ist, genügt für den Zugriff auf die Datenbank im Grunde der Username. Insoweit bezieht sich die Formulierung "gegebenenfalls Password" auch in den Ansprüchen auf möglicherweise in der Praxis anzutreffende andere Gegebenheiten, bei denen die Eindeutigkeit der Zuordnung erst durch die Kombination Username / Password gegeben sein könnte. Unter Verwendung dieser Identitätsmerkmale generiert der Server das Zertifikat, wobei dies in einer Abfolge mehrerer Verfahrensschritte und in einem Dialog mit dem Client im Wesentlichen wie folgt geschieht: Der Server generiert zunächst einen partiellen Zertifikats-Request (in der Regel eine HTML-Seite, welche die die Identitätsmerkmale repräsentierenden Daten enthält und zur Generierung des endgültigen Requests herangezogen wird), den er an den Nutzer sendet. Dieser muss nun noch sein Schlüsselpaar generieren (i.d.R. durch den Browser nach Drücken eines Buttons auf der HTML-Seite), den Identitätsmerkmalen den öffentlichen Schlüssel hinzufügen und das Ganze mit Hilfe des privaten Schlüssels signieren. (Das Format eines solchen Requests wird z.B. im Standard PKCS#10 genauer spezifiziert: <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-10/index.html>.) Dieser signierte Datensatz wird an den Server zurückgesendet, der daraus schließlich das eigentliche Zertifikat (z.B. nach dem X.509-Standard) generiert. Zum Gewinnen zusätzlicher Sicherheit kann es bei dieser Verfahrensweise vorgesehen werden, daß der Server vom Nutzer nochmals das Password abfragt, z.B. vor Generierung des Zertifikatsrequests oder aber zumindest vor der Übermittlung des Zertifikats an den Client.

[0010] Das erfindungsgemäße Verfahren ist jedoch auch unter Verwendung anderer Authentisierungsvarianten bzw. anderer Anmeldeprozeduren möglich. Bei der Durchführung im IP-Netz ist hierbei vorzugsweise auch an die Verwendung des Challenge and Response Authentication Protocol (CHAP) zu denken. Hierbei wird ein ein Zertifikat abfordernder Nutzer bei der Einwahl mit seinem Usernamen von dem Server, bei welchem er sich einwählt (also von dem Server eines Internet-serviceproviders, welcher nicht unbedingt mit dem zur Erstellung des Zertifikat dienenden Servers identisch ist - Einwahlserver), aufgefordert, eine zufällige Zahl (Challenge) mit einem geheimen ihm zugewiesenen und dem Betreiber des Einwahlservers bekannten Schlüssel zu verschlüsseln und die Antwort an den Einwahlserver zurückzusenden. Der Einwahlserver verschlüsselt seinerseits die gleiche Zahl mit dem geheimen Schlüssel. Entspricht das dabei erhaltene Ergebnis der Antwort des Nutzers des Clients, war die Anmeldung erfolgreich. Im Ergebnis dieser RADIUS-Abfrage wird dann dem Nutzer des Clients die temporäre Internetadresse zugeteilt. Erst wenn dem Nutzer die temporäre Internetadresse

zugewiesen wurde, kann er sich im IP-Netz bewegen und eine Verbindung zu dem die Zertifikate bereitstellenden Server aufbauen.

[0011] In umgekehrter Weise, in welcher dem Nutzer bzw. dem Client bei der RADIUS-Abfrage die temporäre IP-Adresse zugeteilt wurde, kann der das Zertifikat generierende Server bei einer Zertifikatsanforderung aus der dabei für die Verbindung zu ihm verwendeten temporären IP-Adresse den Usernamen des Nutzers gewinnen und mit diesem mittels einer Datenbankabfrage auf die Identitätsmerkmale des Nutzers zugreifen. Auf Grund des bereits bestehenden Vertragsverhältnisses zwischen dem Nutzer und dem ISP können dabei diese Merkmale als vertrauenswürdig (authentisch) angesehen werden. Folglich kann der Server hieraus ein authentisches elektronisches Zertifikat erstellen und an den Client übertragen. Auch bei der Anmeldung unter Nutzung von CHAP kann eine RADIUS-CHAP-Abfrage zur nochmaligen Authentifizierung des Nutzer erfolgen, bevor das bereits generierte Zertifikat vom Server an den Client übermittelt wird.

Je nach der Struktur im Hinblick auf die Organisation der Zertifizierungsstelle bzw. des den Zugang zum Internet ermöglichenden ISP (Internet-Service-Provider), aber unabhängig von der verwendeten Anmeldeprozedur (PAP oder CHAP), kann es sich bei dem Server, welcher die Zertifikate generiert, um denselben Server handeln, welcher auch den Zugang zum Internet ermöglicht. In jedem Falle handelt es sich aber um einen Server, der auf die Identitätsmerkmale des Nutzers, welche im Rahmen der elektronischen Abbildung seines Vertragsverhältnisses mit dem ISP in einer Datenbank abgespeichert wurden, Zugang hat.

Entsprechend einer vorteilhaften Weiterbildung des Verfahrens ist es vorgesehen, dass die Generierung eines Zertifikats durch einen hierfür bestimmten Server erst dann erfolgt, wenn das elektronisch abgebildete Vertragsverhältnis und die zu diesem Zweck abgespeicherten Identitätsmerkmale bereits über einen vorbestimmten Zeitraum in der Datenbank abgelegt sind. Im Beispiel des Vertragsverhältnisses mit einem ISP könnte es also denkbar sein, den Daten ein Kennzeichen zuzuordnen, durch welches sie erst nach ein oder zwei Abrechnungsperioden, in denen der ISP die anfallenden Internetgebühren beim Nutzer abgerechnet und dabei über die Authentizität des Nutzers auf Grund einer erfolgten Zahlung höhere Sicherheit gewonnen hat, zur Erstellung eines Zertifikats zugelassen werden. In Fällen, bei denen das Datum des Vertragsabschlusses sowieso erfasst und in der Datenbank gespeichert wird, bedarf es nicht einmal eines solchen zusätzlichen Merkmals. Vielmehr muss der mit der Erzeugung des Zertifikats beauftragte Server nach dem Eingang der aus der Datenbank abgeforderten Nutzerangaben nur dieses Datum überprüfen und entsprechend des Ergebnisses eines Vergleichs mit einer voreingestellten zeitlichen Bedingung das Zertifikat generieren oder dessen Generierung verweigern. Für den Fachmann ist klar, dass ein

solches zusätzliches, praktisch einer Plausibilitätsabfrage entsprechendes Kriterium ohne weiteres unter Nutzung der (des) von den Servern geführten internen Systemzeit (-datums) ausgewertet werden kann.

[0012] Die Erfindung soll nachfolgend nochmals an einem Beispiel verdeutlicht werden.

[0013] Ein Internetnutzer hat ein bestehendes Vertragsverhältnis mit einem ISP. In einer Datenbank auf einem Server des ISP sind bestimmte im Zusammenhang mit dem Abschluss des Vertrages bei dem Nutzer erhobene Identitätsmerkmale abgespeichert. Diese werden durch die Einwahl des Nutzers in das Internet nach dem erfolgreichen Durchlaufen einer Anmeldeprozedur zugänglich. Der Nutzer wird beispielsweise bei der Anmeldung, sofern diese nach der PAP-Methode erfolgt, nach seinem Nutzernamen und dem Passwort gefragt. Im Zuge der RADIUS-Abfrage wird schließlich dem Client des Nutzers eine temporäre Internetadresse zugeordnet. Der Nutzer baut nun von seinem Client aus eine Internet-Verbindung zu einem Server einer Zertifizierungsstelle auf und fordert dort ein elektronisches Zertifikat ab. Auf Grund dessen, dass dieser Server ebenfalls durch den ISP oder aber in seinem Auftrage betrieben wird, hat der Server Zugriff auf die RADIUS-Nutzerdaten und die Kundendatenbank des ISP. Ein solcher RADIUS-Nutzereintrag sieht beispielsweise wie folgt aus:

```
user_x Password = "abcde", Caller-Id =
"00892225558"
Ascend-Send-Auth = Send-Auth-PAP,
Framed-Protocol = PPP,
User-Service = Framed-User,
Framed-Address = 141.45.240.1.,
Framed-Netmask = 255.255.255.255,
Ascend-Metric = 2,
Framed-Routing = None,
Ascend-Idle-Limit = 720,
Ascend-Dial-Number = 00892225558
```

[0014] Im Sinne einer inversen RADIUS-Abfrage löst der das Zertifikat generierende Server die temporäre Internetadresse (141.45.240.1.) zunächst zu Username (user_x) und gegebenenfalls zu Password (vorliegend "abcde") des Nutzers auf. Mit diesen Angaben kann er nun über eine Datenbankabfrage bei der Datenbank, in welcher der ISP seine Kundendaten als elektronische Abbildung der mit den Kunden geschlossenen Verträge hinterlegt hat, als Identitätsmerkmale des das Zertifikat anfordernden Nutzers abrufen. In Bezug auf die an den entsprechenden ISP vertraglich gebundenen Nutzer ist dabei durch den Usernamen bzw. die Kombination Username/Password eine eindeutige Zuordnung zu bestimmten Kundendaten (Merkmalen) gegeben. Diese Merkmale, welche auf Grund des möglicherweise bereits länger bestehenden Vertragsverhältnisses zwischen dem Nutzer und dem ISP als authentisch einzustufen sind, nimmt der zur Bereitstellung des Zertifikats

aufgeforderte Server zur Grundlage für die Generierung desselben. Mittels einer Einweg-Hash-Funktion erzeugt er das entsprechende Zertifikat. Nach der Generierung des Zertifikats oder parallel dazu wird der Nutzer über seinen Client durch den mit ihm in Verbindung stehenden Server nochmals zur Eingabe von User-Name und Password aufgefordert. Werden diese Angaben korrekt an den Server übermittelt, dann überträgt dieser das den Nutzer eindeutig authentisierende elektronische Zertifikat an dessen Client. Der Nutzer verfügt nun über ein Zertifikat, das er einerseits zur authentischen Übermittlung seines öffentlichen Schlüssels an Dritte, und andererseits zum Nachweis der Authentizität einer von ihm mit seinem privaten Schlüssel generierten Signatur verwenden kann. Durch das Vertrauen, welches die Nutzer in die Zertifizierungsbehörde haben, die den die Zertifikate generierenden Server unterhält, ergibt sich gleichzeitig das Vertrauen in die Authentizität des jeweils verwendeten Zertifikats.

Patentansprüche

1. Verfahren zur Bereitstellung eines authentischen elektronischen Zertifikats, bei dem ein solches Zertifikat von einem Client unter Nutzung einer elektronischen Verbindung von einem in eine Public Key-Infrastruktur eingebundenen Server abgefordert, von dem Server automatisch generiert und an den Client übertragen wird, wobei der Server das Zertifikat unter Nutzung von Identitätsmerkmalen generiert, welche in seinem Speicher oder in Speichermedien, auf die er über elektronische Verbindungen Zugriff hat, auf der Grundlage eines bestehenden, in dem Speicher oder den Speichermedien elektronisch abgebildeten Vertragsverhältnisses gespeichert und im Hinblick auf das bestehende Vertragsverhältnis als vertrauenswürdig (authentisch) einzustufen sind, sowie aufgrund einer der Verbindung mit dem Server vorangegangenen Anmeldeprozedur als Voraussetzung für den Aufbau dieser elektronischen Verbindungen durch den Client in einer zumindest vermeintlich eindeutigen Zuordnung zu einem das Zertifikat mittels des Clients abfordern den Nutzer stehen.
2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** es sich bei der elektronischen Verbindung zwischen dem Server und dem Client um eine IP-Verbindung handelt.
3. Verfahren nach Anspruch 2, **dadurch gekennzeichnet, dass** die dem Client bei der Einwahl in das IP-Netz nach dem erfolgreichen Durchlaufen einer Anmeldeprozedur zugeteilte temporäre IP-Adresse als zentraler technischer Referenzwert für den Zugriff des das Zertifikat generierenden Servers auf die im Zuge der elektronischen Abbildung

- des bestehenden Vertragsverhältnisses gespeicherten Identitätsmerkmale dient.
4. Verfahren nach Anspruch 3, **dadurch gekennzeichnet, dass** der Zugriff des Servers auf die Identitätsmerkmale unter Umkehr der bei der Einwahl des Clients in das IP-Netz für die Zuweisung der temporären IP-Adresse genutzten Remote Authentication Dial-In User Service-Abfrage (RADIUS-Abfrage) erfolgt, wobei der Server die temporäre IP-Adresse, unter der er kontaktiert wurde, durch eine inverse RADIUS-Abfrage und eine sich anschließende Datenbankabfrage zu den authentischen Daten des Nutzers hin auflöst.
5
10
15
 5. Verfahren nach Anspruch 3 oder 4, **dadurch gekennzeichnet, dass** die Anmeldung des den Client bedienenden Nutzers bei der Einwahl in das IP-Netz unter Verwendung der Password Authentication Protocol-Methode (PAP) erfolgt und der das Zertifikat generierende Server, die dem Nutzer nach der Anmeldung zugeteilte temporäre IP-Adresse im Zuge der inversen RADIUS-Abfrage zunächst zu Username und gegebenenfalls Password auflöst und unter Nutzung dieser Angaben Zugriff auf die in der Datenbank hinterlegten Identitätsmerkmale des Nutzers erhält.
20
25
 6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, dass** der das Zertifikat generierende Server im Zuge der Generierung, jedoch zumindest vor der Übertragung des Zertifikats an den Client, nochmals das zur Einwahl in das IP-Netz und mit dem elektronisch abgebildeten Vertragsverhältnis und dem Usernamen korrespondierende Password beim Nutzer abfordert.
30
35
 7. Verfahren nach Anspruch 3 oder 4, **dadurch gekennzeichnet, dass** die Anmeldung des den Client bedienenden Nutzers bei der Einwahl in das IP-Netz unter Verwendung der Challenge and Respond Authentication Protocol-Methode (CHAP) erfolgt und der das Zertifikat generierende Server, die dem Nutzer nach der Anmeldung zugeteilte temporäre IP-Adresse durch eine inverse RADIUS-Abfrage unter Nutzung der CHAP-Methode und eine sich anschließende Datenbankabfrage hin zu den durch die elektronische Abbildung des Vertragsverhältnisses zu einem Internetserviceprovider (ISP) gespeicherten Identitätsmerkmalen des Nutzers auflöst.
40
45
50
 8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet, dass** der das Zertifikat generierende Server den Nutzer im Zuge der Generierung, jedoch zumindest vor der Übertragung des Zertifikats, nochmals mit einer CHAP-Abfrage überprüft.
55
 9. Verfahren nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet, dass** die Generierung des Zertifikats erst nach einer bestimmten Zeit des Bestehens des Vertragsverhältnisses zugelassen wird.